What is claimed is:

1. A data processing method performed by a computer, comprising:

a first step for specifying a plurality of linear conversion candidates respectively satisfying a restriction on a circuit for realizing linear conversion;

a second step for specifying for each of said plurality of linear conversion candidates specified in said first step a minimum value of the number of zeros arisen in respective results of performing linear conversion restricted by the linear conversion candidates on a plurality of input data; and

a third step for specifying said linear conversion candidate wherein said minimum value specified in said second step becomes largest among said plurality of linear conversion candidates specified in said first step.

2. A data processing method as set forth in claim 1, wherein:

said first step specifies as said plurality of linear conversion candidates linear conversion which is a combination of a plurality of unit linear conversions wherein one of two zero regions in a

replacing matrix is replaced by a conversion matrix; and

said second step specifies said minimum value for each of said linear conversion candidates obtained by giving a plurality of different matrixes as said conversion matrixes of said plurality of unit linear conversion.

3. A data processing method as set forth in claim 2, wherein:

the number of said plurality of unit linear conversion is M; and

said unit linear conversion is realized by calculation of a matrix of M by M.

4. A data processing method as set forth in claim 3, wherein said first step defines said linear conversion candidates by a formula (1) below by using conversion matrixes C_1, C_2, C_3 and C_4.

$$\begin{pmatrix} I + C_4C_3 + C_2C_1 + C_4C_3C_2C_1 + C_4C_1 & C_2 + C_4C_3C_2 + C_4 \\ C_3 + C_3C_2C_1 + C_1 & I + C_3C_2 \end{pmatrix} \quad \cdots (1)$$

5. A data processing method as set forth in claim 1, wherein

when said linear conversion is a linear conversion restricted in round function processing of common key block encryption, said second step performs said linear conversion on said input data obtained by performing nonlinear diffusion processing on a plain data.

6. A data processing method as set forth in claim 1, further comprising a fourth step for configuring a linear conversion circuit having a circuit block for realizing said unit linear conversion corresponding to said linear conversion candidates specified in said third step.

7. A program to be executed by a computer, comprising:

a first procedure for specifying a plurality of linear conversion candidates respectively satisfying a restriction on a circuit for realizing linear conversion;

a second procedure for specifying for each of said plurality of linear conversion candidates specified in said first procedure a minimum value of the number of zeros arisen in respective results of performing linear conversion restricted by the linear conversion candidates on a plurality of input data; and

a third procedure for specifying said linear

conversion candidate wherein said minimum value specified in said second procedure becomes largest among said plurality of linear conversion candidates specified in said first procedure.

8. A program as set forth in claim 7, wherein:

said first procedure specifies as said plurality of linear conversion candidates linear conversion which is a combination of a plurality of unit linear conversions wherein one of two zero regions in a replacing matrix is replaced by a conversion matrix; and

said second procedure specifies said minimum value for each of said linear conversion candidates obtained by giving a plurality of different matrixes as said conversion matrixes of said plurality of unit linear conversion.

9. A data processing apparatus, comprising:

a first means for specifying a plurality of linear conversion candidates respectively satisfying a restriction on a circuit for realizing linear conversion;

a second means for specifying for each of said plurality of linear conversion candidates specified in said first means a minimum value of the number of zeros arisen in respective results of performing linear

conversion restricted by the linear conversion candidates on a plurality of input data; and

a third means for specifying said linear conversion candidate wherein said minimum value specified in said second means becomes largest among said plurality of linear conversion candidates specified in said first means.

10. A linear conversion circuit for performing linear conversion defined in round function processing of common key block encryption, comprising

a plurality of data lines corresponding respectively to a plurality of data; and

a plurality of circuit blocks for performing linear conversion successively on said plurality of data input via said plurality of data lines;

wherein each of said circuit blocks comprises a calculation circuit provided on a part of said plurality of data lines among said plurality of data lines and is configured so that data is supplied to at most one of said calculation circuits from said data lines not provided with a calculation circuit.

11. A linear conversion circuit as set forth in claim 10, wherein, when said plurality of data lines are

divided to a first data line group and a second data line group having the same number, each of said circuit blocks comprises said calculation circuit only on data lines in said first data line group and is configured so that data is output from data lines in said second data line group to said calculation circuit in said first data line group.

12. An encryption apparatus for performing common key block encryption by performing round function processing, comprising:

a non linear conversion circuit for performing nonlinear conversion defined in said round function processing; and

a linear conversion circuit for performing linear conversion on input data subjected to said nonlinear conversion by said nonlinear conversion circuit;

wherein:

said linear conversion circuit comprises

a plurality of data lines corresponding respectively to a plurality of data composing said input data; and

a plurality of circuit blocks for performing linear conversion successively on said plurality of data input via said data lines; and

each of said circuit blocks comprises a calculation circuit provided on a part of said plurality of data lines among said plurality of data lines and is configured so that data is supplied to at most one of said calculation circuits from said data lines not provided with a calculation circuit.